Commonwealth of Kentucky
Cabinet for Health and Family Services

Cabinet for Health and Family Services (CHFS) Information Technology (IT) Policy

050.102 Information Systems Security Incident Response and Reporting

Version 2.3
May 2, 2018

Revision History

Date	Version	Description	Author
10/1/2006	1.0	Effective Date	CHFS IT Policies Team Charter
5/2/2018	2.3	Revision Date	CHFS OATS Policy Charter Team
5/2/2018	2.3	Review Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
CHFS IT Executive (or designee)	5/2/2018	Jennifer L. Harp	Jennifer L. Harp
CHFS Chief Information Security Officer (or designee)	5/2/2018	Dennis E. Leber	

Table of Contents

Policy Definitions

- **Confidential Data:** Defined by COT standards, is data of which the Commonwealth has a legal obligation not to disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples would include, but are not limited to, data not releasable under the Kentucky State law, Protected Health Information, Federal Tax Information, and Social Security and Credit Card Numbers.
- **Contract Staff/Personnel:** An employee hired through a state approved (i.e. SDS Vendor Agreement/Company) vendor who has a master agreement with the state.
- **Personally Identifiable Information:** Per the Health Insurance Portability and Accountability Act (HIPAA) definition, a subset of health information that is collected from an individual. This information can also be created or received by a health care provider, health plan, public health authority, employer, or other source that relates to physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. This is information that can be used to distinguish or identify an individual or can be used to identify an individual. Examples include, but are not limited to: Name, Social Security Number, Biometric Records, etc.
- **Protected Health Information:** Per the HIPAA definition, Protected Health Information (PHI) is any Personally Identifiable Information (PII) that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. This is information that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. Examples include but are not limited to: Hospital Billing Information, Phone Records, Medical Test Results, etc.
- **Federal Tax Information:** Per Internal Revenue Services (IRS) definition, any information that is received from the IRS or secondary source, such as the Social Security Administration (SSA), Federal Office of Child Support Enforcement or Bureau of Fiscal Service. Examples include but are not limited to: Tax Returns received from a federal source, Information regarding Taxpayers' Account Information, Information Extracted from a Tax Return such as Social Security Number, Employer Identification Number, etc.
- **Security Breach:** Per Kentucky Revised Statute (KRS) Chapter 61, the unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of encrypted or unencrypted records or data that compromises the security, confidentiality, or integrity of another's personal information or confidential information that result in the likelihood of harm to one (1) or more individuals.

- **Sensitive Data:** Defined by COT standards, is data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include, but are not limited to, information identifiable to an individual (i.e. dates of birth, driver's license numbers, employee ID numbers, license plate numbers, and compensation information) and Commonwealth proprietary information (i.e. intellectual property, financial data, and more.)
- **State Staff/Personnel:** An employee hired directly through the state within the CHFS.
- **Vendor Staff/Personnel:** An employee contracted through an approved Master Business Associate Agreement, or other formal agreement, to provide temporary work for CHFS.

050.102 Information Systems Incident Response and Reporting

Category: 050.000 Security Awareness

1 Policy Overview

1.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish an acceptable level of security controls to be implemented through an incident response and reporting policy. This document establishes the agency's Information Systems Incident Response and Reporting Policy to manage risks and provide guidelines for security best practices regarding responding to and reporting security incidents.

1.2 Scope

The scope of this policy applies to all internal CHFS employees, consultants, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems. External vendors or other defined groups/organizations providing information security or technology services may work with the CHFS agency(s) to request exceptions to this policy.

1.3 Management Commitment

This policy has been approved by OATS Division Directors, CHFS Chief Technical Officials, and Office of the Secretary IT Executive. Senior Management supports the objective put into place by this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of CHFS property (physical or intellectual) are suspected, CHFS may report such activities to the appropriate authorities.

1.4 Coordination among Organizational Entities

OATS coordinates with other organizations or agencies within the Cabinet with access to applications or systems. All organizational entities that interact with CHFS systems, within or contracted by OATS, are subject to follow requirements outlined within this policy. External vendors, or other defined groups/organizations, providing information security or technology services may work with the CHFS agency(s) when seeking exceptions to this policy.

1.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Applicable agencies additionally follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

2 Roles and Responsibilities

2.1 Chief Information Security Officer (CISO)

This positon is responsible for the assessment, planning, and implementation of all security standards, practices, and commitments required. This position is responsible to adhere to this policy.

2.2 Security/Privacy Lead

Individual(s) is designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate personnel. This individual(s) is responsible for providing privacy and security guidance for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff and contractor personnel. This is role along with the CHFS OATS Information Security (IS) Team is responsible for the adherence of this policy.

2.3 Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer

An attorney within CHFS Office of Legal Services (OLS) fills the Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer position. This position is responsible for conducting HIPAA mandated risk analysis on information provided by the CISO or CHFS OATS Information Security (IS) Team. The HIPAA Privacy Officer will coordinate with the Information Security Agency Representative, the CISO, or CHFS OATS IS Team, and other CHFS agencies to ensure compliance with HIPAA notification requirements in the event of a breach. This position is responsible for reporting identified HIPAA breaches to Health and Human Services (HHS) Office of Civil Rights (OCR) and keeping records of risk analyses, breach reports, and notifications in accordance with HIPAA rules and regulations.

2.4 CHFS Staff and Contractor Employees

All CHFS staff, contract employees, and other applicable vendor/contract staff must adhere to this policy. All personnel must comply with referenced documents that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

2.5 System Data Owner and System Data Administrators

It is the responsibility of these management/lead positons, to work with the application's development team to document components that are not included in the base server build and ensure backup are conducted in line with business needs. This individual(s) will be responsible to work with Enterprise, agency, and application technical and business staff to provide full recovery of all the application functionality and meet federal and state regulations for disaster recovery situations.

2.6 Office of Attorney General Staff Attorney

The Staff Attorney for the Office of Attorney General oversee that all applicable state laws are followed in reference to reportable breaches.

2.7 Finance and Administration Cabinet Secretary

The Finance and Administration Cabinet Secretary tracks all determined breaches to analyze if there is a possible financial impact.

2.8 Kentucky State Police, Commissioner

The Kentucky State Police Commissioner will need to be informed of a determine breach in the event law enforcement needs to be involved.

2.9 Auditor of Public Accounts

The Auditor of Public Accounts (APA) job function is to audit the entire state government. They shall be notified of any security breach to correlate and determine if the appropriate response or action has been taken.

2.10 Incident Response Coordinator

The Incident Response Coordinator collects the information regarding the incident and disseminates to all relevant parties.

2.11 CHFS Office of Communications

The CHFS Office of Communications shall be updated on all confirmed/determined breaches that results in any media coverage regarding the incident/breach.

2.12 CHFS General Counsel

The CHFS General Counsel would need to be aware of any determined breaches to verify governmental agency reporting processes are followed.

3 Policy Requirements

3.1 General Security Incident Response

Any CHFS employee, contractor, or vendor who suspects an information security incident must report that incident as soon as possible to their supervisor. The employee or supervisor must contact their designated CHFS agency privacy/security liaison/lead, HIPAA privacy officer, or incident coordinator form the contact list (Security IRP Contacts) as well as the CHFS OATS Information Security (IS) Team at CHFSOATSSecurity@ky.gov to provide information for investigation into the event or incident.

If any employee has questions or concerns regarding information security incidents within the Cabinet, they may contact the CHFS OATS IS Team as stated above. After the conclusion of each major incident, a post incident lessons learned report would be completed and made available for management review and action.

3.2 Security Incident Reporting

OATS IS Team uses the Security Incident Tracking SharePoint site to log, investigate and report all security incidents. CHFS adheres to all federal and state requirements regarding the investigation, management and reporting of information security incidents and/or security breaches.

3.3 Health Insurance Portability and Accountability Act (HIPAA)

The Cabinet follows the HIPAA requirements for logging security incidents. Additionally, CHFS investigates potential security breaches as defined under The Health Information Technology for Economic and Clinical Health (HITECH) Act and complies with all reporting requirements as outlined under the HITECH Act. Per the CHFS Business Associate Agreement, the agency must notify the covered entity **within five (5) calendar days** of the discovery of a breach.

When PHI and 499 or fewer records are involved, the Privacy Officer, or designee, must log the incident and report to The HHS website, at least annually. For data breaches of 500 or more records, the Privacy Officer, or designee, must report to the HHS website once the breach and number of records are confirmed.

Within the Public Health domain and all area encompassed, such as Laboratories, there are specific exceptions where PHI can be released without consent from a citizen. These exceptions are detailed in the HIPAA Privacy Rule. Refer to the section titled Permitted PHI Disclosures without Authorization for details that outlines what the precise conditions would be to allow for the release of the PHI.

3.4 Internal Revenue Service (IRS)

The Cabinet follows all security incident requirements for Federal Tax Information (FTI) as outlined in IRS Publication 1075. The Treasury Inspector General for Tax Administration (TIGTA) must be notified immediately, **but no later than twenty-four (24) hours after** the identification of a possible issue involving FTI is discovered. CHFS will contact Kentucky's TIGTA Field Division in Washington at (215) 861-1003.

3.5 Social Security Administration (SSA)

The SSA requires the agency entrusted with SSA supplied with Protected Health Information (PHI) and/or Personally Identifiable Information(PII) data report any suspected or confirmed breach of personal data be reported to their SSA Regional Office Contact and SSA Systems Security Contact **within one (1) hour** of discovery of the incident. If the responsible State official or delegate is unable to notify the SSA Regional Office or the SSA Systems Security Contact within one hour, the responsible State Agency official or delegate must report the incident by contacting SSA's National Network Service Center (NNSC) toll free at 877-697-4889 (select "Security and PII Reporting" from the options list).

The CHFS agency will provide updates as they become available to SSA contact, as appropriate. Refer to the worksheet provided in the agreement to facilitate gathering and organizing information about an incident.

3.6 Kentucky Revised Statues (KRS) 61.931 to 61.933

Kentucky Revised Statues (KRS) Chapter 61 §931 to 933 requires that a state agency or a nonaffiliated third party the agency contracts with must report a personal information security breach to the officials listed in KRS 61.933(1)(a). The notice of the security breach of personal information shall be in the most expedient time possible and without unreasonable delay but **within seventy-two (72) hours** of determination or notification of the security breach. The notification required by KRS 61.933(1)(a) shall include all information the agency (or nonaffiliated third party) has with regard to the security breach at the time of notification.

The officials (Security IRP Contacts) that must be notified by email of a security breach, according to KRS 61.933(1)(a) are as follows:

- Office of Attorney General Staff Attorney
- Finance and Administration Cabinet Secretary
- Kentucky State Police, Commissioner
- Auditor of Public Accounts
- In addition, for CHFS OATS add or forward to:
    - Privacy officer
    - Security Officer
    - Incident Coordinator- Incident Response Coordinator
    - CHFS Office of Communications
    - CHFS General Counsel

3.7 Other Reporting

More examples of the types of incidents and breaches that could be encountered are covered in the COT CIO-090 Information Security Incident Response Policy.

CHFS is committed to ensuring that the employees tasked with handling security incidents are adequately trained and prepared to handle their incident response duties, please refer to the CHFS OATS Incident Response Plan for more information regarding appropriate processes and steps when dealing with potential incidents. CHFS will periodically perform incident response exercises, but at least once annually. The exercises are conducted in part as training exercises as well as to test the incident response process.

3.8 Employee Responsibility

CHFS employees are responsible for reporting security incidents. The following security incidents must be reported:

- Possible or actual exposure release, alteration or loss of confidential information
- Giving or telling another person your password.
- Loss or theft of a laptop or desktop computer or handheld data device.
- Loss or theft of external storage devices, like external hard drives, ZIP and flash drives, CDs and DVDs, used for Cabinet business.
- Loss of employee badge or keys.
- Unauthorized use of CDs, DVDs or other removable media to copy confidential information.
- Attempts to obtain confidential information by e-mail or other electronic communication.
- Attempts by unknown sources to persuade users to download infected e-mail or attachments as well as possible phishing emails.
- Receipt of unsolicited, unusual or suspicious e-mail or phone calls.
- Unauthorized physical entry into a controlled area that contains confidential information.
- Electronic monitoring of another employee’s workstation.

4 Policy Maintenance Responsibility

The OATS IS Team is responsible for the maintenance of this policy.

5 Policy Exceptions

Within the Public Health domain and all area encompassed, such as Laboratories, there are specific exceptions when PHI can be released without consent from a citizen.

These exceptions are detailed in the HIPAA Privacy Rule. The section titled Permitted PHI Disclosures without Authorization outlines what the precise conditions would be to allow for the release of the PHI. All other exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

6 Policy Review Cycle

This policy is reviewed at least once annually, and revised on an as needed basis.

7 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS OATS Incident Response Plan
- CHFS OATS Policy: 010.102- Data/Media Security Policy
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- Enterprise IT Policy: CIO-085- Authorized Agency Contacts Policy
- Enterprise IT Policy: CIO-090- Information Security incident Response Policy
- Enterprise IT Policy: CIO-091- Enterprise Information Security Program Policy
- Employee Privacy and Security of Protected Health, Confidential, and Sensitive Information Agreement- CHFS 219 Form
- OHRM Personnel Handbook
- Internal Revenue Services (IRS) Publication 1075
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Security Incident Response Plan (IRP) Contacts
- Social Security Administration (SSA) Security Information